What is claimed is:

1. A method for reducing the occurrence of unauthorized use of on-line resources, comprising:

receiving a message indicating a request from a user to use on-line resources;

determining whether the request requires authentication;

obtaining an indicia of physical identification from the user if authentication is required;

comparing the obtained indicia to a stored indicia for the user; and

enabling the request to be fulfilled if the obtained indicia matches the stored indicia.

2. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether a stored profile for the user indicates that authentication is required.

3. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether stored business rules for a company associated with the requested on-line resource indicates that authentication for the user is required.

4. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as always requiring authentication; and

requiring authentication if the user is listed.

5. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as never requiring authentication; and

not requiring authentication if the user is listed.

6. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as being completely denied access; and

completely denying access to the requested on-line resources if the user is listed.

7. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether the request is indicative of fraudulent behavior.

8. A method according to claim 7, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

9. A method according to claim 1, further comprising determining whether the request satisfies other criteria of authorization if authentication is not required.

10. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

determining whether the request is a card transaction;

determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

denying the request if the restrictions are not satisfied.

11. A method according to claim 10, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

12. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

determining whether the request is an account transaction;

determining whether restrictions applied to an account associated with the account

transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

13. A method according to claim 12, wherein the restrictions are one or more of frequency of access and time of access.

14. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

determining whether the request is an account transaction;

determining whether use of the requested on-line resources are restricted for an account associated with the user; and

denying the request if the requested on-line resources are restricted for the account.

15. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

determining whether the request is a control transaction;

determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

16. A method according to claim 15, wherein the restrictions are one or more of a parent

control and an other control.

17. A method according to claim 1, wherein the indicia is a biometric.

18. A method according to claim 17, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

19. A method according to claim 1, further comprising configuring a set of rules that are used in the determining step.

20. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

means for receiving a message indicating a request from a user to use on-line resources;

means for determining whether the request requires authentication;

means for obtaining an indicia of physical identification from the user if authentication is required;

means for comparing the obtained indicia to a stored indicia for the user; and

means for enabling the request if the obtained indicia matches the stored indicia.

21. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether a stored profile for the user indicates that authentication is required.

22. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether a stored profile for a company associated with the requested on-line resource indicates that authentication for the user is required.

23. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as always requiring authentication; and

means for requiring authentication if the user is listed.

24. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as never requiring authentication; and

means for not requiring authentication if the user is listed.

25. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as being completely denied access; and

means for completely denying access to the requested on-line resources if the user is listed.

26. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether the request is indicative of fraudulent behavior.

27. An apparatus according to claim 26, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

28. An apparatus according to claim 20, further comprising means for determining whether the request satisfies other criteria of authorization if authentication is not required.

29. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

means for determining whether the request is a card transaction;

means for determining whether restrictions applied to the user and an account

associated with the request are satisfied by a purchase associated with the request; and

means for denying the request if the restrictions are not satisfied.

30. An apparatus according to claim 29, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

31. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

means for determining whether the request is an account transaction;

means for determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

32. An apparatus according to claim 31, wherein the restrictions are one or more of frequency of access and time of access.

33. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

means for determining whether the request is an account transaction;

means for determining whether use of the requested on-line resources are restricted for an account associated with the user; and

means for denying the request if the requested on-line resources are restricted for the account.

34. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

means for determining whether the request is a control transaction;

means for determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

35. An apparatus according to claim 34, wherein the restrictions are one or more of a parent control and an other control.

36. An apparatus according to claim 20, wherein the indicia is a biometric.

37. An apparatus according to claim 36, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

38. An apparatus according to claim 20, further means for configuring a set of rules that are used by the determining means.

39. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

a server that is adapted to communicate with a network based service so as to receive a message indicating a request from a user to use the network based service;

a rules subsystem coupled to the server that determines whether the request requires authentication, and causes the server to obtain an indicia of physical identification from the user if authentication is required; and

an authentication subsystem coupled to the server and the controller that compares the obtained indicia to a stored indicia for the user,

wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia.

40. An apparatus according to claim 39, further comprising a database coupled to the controller, the controller accessing historical rules from the database to determine whether authentication is required for the user for a current transaction.

41. An apparatus according to claim 39, further comprising a database coupled to the controller, the controller accessing business rules from the database to determine whether a company associated with the requested on-line resource requires authentication for the user.

42. An apparatus according to claim 39, further comprising a user profile subsystem coupled to the controller which is adapted to determine whether the request is indicative of fraudulent behavior.

43. An apparatus according to claim 42, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

44. An apparatus according to claim 39, wherein the indicia is a biometric, the apparatus further comprising a database that stores a plurality of biometrics for a respective plurality of users.

45. An apparatus according to claim 44, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.